Field reduction and linear sets in finite geometry

Michel Lavrauw * Geertrui Van de Voorde *

April 2, 2014

Abstract

Based on the simple and well understood concept of subfields in a finite field, the technique called 'field reduction' has proved to be a very useful and powerful tool in finite geometry. In this paper we elaborate on this technique. Field reduction for projective and polar spaces is formalised and the links with Desarguesian spreads and linear sets are explained in detail. Recent results and some fundamental questions about linear sets and scattered spaces are studied. The relevance of field reduction is illustrated by discussing applications to blocking sets and semifields.

Keywords: field reduction, Desarguesian spread, Segre variety, linear set, scattered spaces

1 Introduction

In the last two decades a technique, commonly referred to as 'field reduction', has been used in many constructions and characterisations in finite geometry. This is somehow surprising since the technique is based on the well known structure of subfields of a finite field. In this paper we will elaborate on this technique and explain how such a simple idea gives rise to highly non-trivial constructions and characterisations of geometric and algebraic structures.

For projective spaces the idea goes back to the 1960's, when B. Segre introduced Desarguesian spreads arising from field reduction [42]. At the end of the 1990's, the link with *linear sets* was introduced which renewed the interest for this technique, because it turned out to be very useful in the construction and characterisation of different kinds of objects in finite geometry. Field reduction for polar spaces was also introduced in the 1990's, in the study of m-systems [43].

Notation. An n-dimensional vector space over the finite field with q elements $\mathbb{F}_q$ is denoted by $\mathrm{V}(n,q)$ or $\mathbb{F}_q^n$. The $(n-1)$-dimensional projective space corresponding to $\mathrm{V}(n,q)$ is denoted by $\mathrm{PG}(n-1,q)$ or $\mathrm{PG}(\mathbb{F}_q^n)$. A point in $\mathrm{PG}(n-1,q)$ corresponding a nonzero vector $v=(x_0,\ldots,x_{n-1})$ of $\mathrm{V}(n,q)$ is denoted by $\mathbb{F}_q(x_0,\ldots,x_{n-1})$ or $\mathbb{F}_q v$, reflecting the fact that every $\mathbb{F}_q$-multiple of v defines the same projective point in $\mathrm{PG}(n-1,q)$. If U is a subspace of $\mathbb{F}_q^n$, then we denote the corresponding projective subspace of $\mathrm{PG}(n-1,q)$ by $\mathrm{PG}(U)$.

*This author is supported by the Fund for Scientific Research Flanders (FWO – Vlaanderen).

The paper is organised as follows: in Section 2, we formalise field reduction for projective spaces and explain the connection with Desarguesian spreads and Segre varieties. In Section 3, we explain the technique for classical polar spaces, embedded in projective spaces. In Section 4, we turn our attention to linear sets and finally we discuss two topics in which linear sets and field reduction play an important role: blocking sets (Section 5) and semifields (Section 6).

2 Field reduction for projective spaces

The structure of subfields of a finite field is well understood and it is well-known that we can consider the finite field with q^t elements $\mathbb{F}_{q^t}$ as a t-dimensional vector space over $\mathbb{F}_q$. A point $\mathbb{F}_{q^t}v$ of $\mathrm{PG}(r-1,q^t)$ is a 1-dimensional subspace of $\mathbb{F}_{q^t}^r$ and consists of the set of vectors $S_v := \{\alpha v \ : \ \alpha \in \mathbb{F}_{q^t}\}$. Now consider $\mathbb{F}_{q^t}^r$ as a vector space V over $\mathbb{F}_q$. This means that V is defined as the set of vectors of $\mathbb{F}_{q^t}^r$, addition is as in $\mathbb{F}_{q^t}^r$, and so is scalar multiplication but the field of scalars is $\mathbb{F}_q$ instead of $\mathbb{F}_{q^t}$. Observe that V has dimension rt, and clearly the set S_v forms a t-dimensional subspace of V. More generally, let π be a $(k-1)$-dimensional subspace of $\mathrm{PG}(r-1,q^t)$, with $k \in \{0,1,\ldots,r-1\}$. Suppose $\pi = \mathrm{PG}(U)$ with $U = \langle u_1,\ldots,u_k\rangle$. The set of vectors belonging to U is

$$S_U = \{\alpha_1 u_1 + \ldots + \alpha_k u_k \ : \ \alpha_1,\ldots,\alpha_k \in \mathbb{F}_{q^t}\}.$$

Then clearly the set S_U forms a subspace of V of dimension kt. Summarizing we have the following.

Lemma 2.1. *Each $(k-1)$-dimensional subspace $\pi = \mathrm{PG}(U)$ of $\mathrm{PG}(r-1,q^t)$ corresponds to a $(kt-1)$-dimensional subspace $\mathcal{K}(\pi)$ of $\mathrm{PG}(V) \cong \mathrm{PG}(rt-1,q)$ defined by the kt-dimensional subspace of V spanned by the vectors of S_U.*

This is the idea behind *field reduction*. We formalise this idea introducing the *field reduction map* $\mathcal{F}_{r,t,q}$, defined as a map from the subspaces of $\mathrm{PG}(r-1,q^t)$ to the subspaces of $\mathrm{PG}(rt-1,q)$:

$$\mathcal{F}_{r,t,q} : \mathrm{PG}(r-1,q^t) \to \mathrm{PG}(rt-1,q) \ : \ \pi \mapsto \mathcal{K}(\pi), \tag{1}$$

where $\mathcal{K}(\pi)$ is as in the above Lemma. We collect the properties of the field reduction map in the following lemma. The proof easily follows from the definitions but we include a proof to get used to the notation.

Lemma 2.2. *Let $\mathcal{P}$ denote the set of points of $\mathrm{PG}(r-1,q^t)$, and consider $\mathcal{F}_{r,t,q}$ as defined in (1).*
(i) The field reduction map $\mathcal{F}_{r,t,q}$ is injective.
(ii) If π is a $(k-1)$-dimensional subspace of $\mathrm{PG}(r-1,q^t)$, then $\mathcal{F}_{r,t,q}(\pi)$ has dimension $kt-1$, so each subspace contained in the image of $\mathcal{F}_{r,t,q}$ has dimension $kt-1$ for some $k \in \{0,1,\ldots,r-1\}$.
(iii) Any two distinct elements of $\mathcal{F}_{r,t,q}(\mathcal{P})$ are disjoint.
(iv) Each point in $\mathrm{PG}(rt-1,q)$ is contained in an element of $\mathcal{F}_{r,t,q}(\mathcal{P})$.
(v) $|\mathcal{F}_{r,t,q}(\mathcal{P})| = (q^{rt}-1)/(q^t-1)$.
(vi) The intersection of elements in the image of $\mathcal{F}_{r,t,q}$ also belongs to the image of $\mathcal{F}_{r,t,q}$.
(vii) The span of elements in the image of $\mathcal{F}_{r,t,q}$ is either the trivial subspace or can be written as the span of elements of $\mathcal{F}_{r,t,q}(\mathcal{P})$.

Proof. (i) Suppose that $\mathcal{F}_{r,t,q}(\pi_1) = \mathcal{F}_{r,t,q}(\pi_2)$, with $\pi_1 = \mathrm{PG}(U_1)$ and $\pi_2 = \mathrm{PG}(U_2)$, then $S_{U_1} = S_{U_2}$, which implies that $U_1 = U_2$ and $\pi_1 = \pi_2$.

(ii) Every S_U contains q^{kt} vectors forming a vector space of dimension kt over $\mathbb{F}_q$.

(iii) Suppose that $\mathcal{F}_{r,t,q}(P_1)$ and $\mathcal{F}_{r,t,q}(P_2)$, where $P_1 = \mathbb{F}_{q^t}v$ and $P_2 = \mathbb{F}_{q^t}w$ have a point in common, then $\alpha v = \beta w$, which implies that $S_v = S_w$, hence $\mathcal{F}_{r,t,q}(P_1) = \mathcal{F}_{r,t,q}(P_2)$.

(iv) Let P be a point in $\mathrm{PG}(rt-1,q)$, say $P = \mathbb{F}_q w$, then P belongs to $\mathcal{F}_{r,t,q}(\mathbb{F}_{q^t}w)$.

(v) This follows from (i) and (iii).

(vi) The intersection of $\mathcal{F}_{r,t,q}(\pi_1)$ and $\mathcal{F}_{r,t,q}(\pi_2)$ is clearly equal to $\mathcal{F}_{r,t,q}(\pi_1 \cap \pi_2)$.

(vii) If $\pi_1 = \langle P_1, \ldots, P_l\rangle$ and $\pi_2 = \langle P_{l+1}, \ldots, P_s\rangle$, then

$$\langle \mathcal{F}_{r,t,q}(\pi_1), \mathcal{F}_{r,t,q}(\pi_2)\rangle = \langle \mathcal{F}_{r,t,q}(P_1), \ldots, \mathcal{F}_{r,t,q}(P_s)\rangle.$$

□

2.1 Desarguesian spreads

A $(t-1)$-*spread* in $\mathrm{PG}(n-1,q)$ is a set of $(t-1)$-spaces, partitioning the set of points in $\mathrm{PG}(n-1,q)$. Two spreads $\mathcal{S}_1$ and $\mathcal{S}_2$ in $\mathrm{PG}(n-1,q)$ are *equivalent* if there exists a collineation of $\mathrm{PG}(n-1,q)$ mapping one to the other. The following theorem of Segre gives a necessary and sufficient condition for the existence of a $(t-1)$-spread in $\mathrm{PG}(n-1,q)$. We include a proof using the field reduction map.

Theorem 2.3. *[42] There exists a $(t-1)$-spread in $\mathrm{PG}(n-1,q)$ if and only if t divides n.*

Proof. If there exists a $(t-1)$-spread in $\mathrm{PG}(n-1,q)$, it is clear that the number of points in a $(t-1)$-space has to divide the number of points in $\mathrm{PG}(n-1,q)$. From this, it follows that t has to divide n. Conversely, suppose $n = rt$. Put

$$\mathcal{D}_{r,t,q} := \mathcal{F}_{r,t,q}(\mathcal{P}) \tag{2}$$

where $\mathcal{F}_{r,t,q}$ is defined as in (1) and $\mathcal{P}$ denotes the set of points of $\mathrm{PG}(r-1,q^t)$. Then (ii), (iii) and (iv) of Lemma 2.2 imply that $\mathcal{D}_{r,t,q}$ is a $(t-1)$-spread of $\mathrm{PG}(rt-1,q)$. □

A spread $\mathcal{S}$ in $\mathrm{PG}(n-1,q)$ is called *Desarguesian* if there exist natural numbers r and t such that $n = rt$ and $\mathcal{S}$ is equivalent to $\mathcal{D}_{r,t,q}$.

Remark 1. By [42] a $(t-1)$-spread in $\mathrm{PG}(n-1,q)$, where t is a divisor of n, can be also constructed as follows. Embed $\mathrm{PG}(rt-1,q)$ as a subgeometry of $\mathrm{PG}(rt-1,q^t)$ in the canonical way, i.e. by restricting the coordinates to $\mathbb{F}_q$. Let σ be the automorphic collineation of $\mathrm{PG}(rt-1,q^t)$ induced by the field automorphism $x \to x^q$ of $\mathbb{F}_{q^t}$, i.e., $\sigma : \mathbb{F}_{q^t}(x_0, x_1, \ldots, x_{rt-1}) \mapsto \mathbb{F}_{q^t}(x_0^q, x_1^q, \ldots, x_{rt-1}^q)$. Then σ fixes $\mathrm{PG}(rt-1,q)$ pointwise and one can prove that a subspace of $\mathrm{PG}(rt-1,q^t)$ of dimension d is fixed by σ if and only if it intersects the subgeometry $\mathrm{PG}(rt-1,q)$ in a subspace of dimension d and that there exists an $(r-1)$-space π skew to the subgeometry $\mathrm{PG}(rt-1,q)$ (see [11]). Let P be a point of π and let $L(P)$ denote the $(t-1)$-dimensional subspace generated by the conjugates of P, i.e., $L(P) = \langle P, P^\sigma, \ldots, P^{\sigma^{t-1}}\rangle$. Then $L(P)$ is fixed by σ and hence it intersects $\mathrm{PG}(rt-1,q)$ in a $(t-1)$-dimensional subspace over $\mathbb{F}_q$. Repeating this for every point of π, one obtains a set $\mathcal{S}$ of $(t-1)$-spaces of the subgeometry $\mathrm{PG}(rt-1,q)$ forming a spread. This spread is equivalent to $\mathcal{D}_{r,t,q}$.

A *regulus* in a projective space, or $(t-1)$-*regulus* if we want to specify the dimension of the elements, is a set $\mathcal{R}$ of $q+1$ two by two disjoint $(t-1)$-spaces with the property that each line meeting three elements of $\mathcal{R}$ meets all elements of $\mathcal{R}$. If S_1, S_2, S_3 are mutually disjoint $(t-1)$-subspaces with $\dim\langle S_1, S_2, S_3\rangle = 2t-1$, then there is a unique regulus $\mathcal{R}(S_1, S_2, S_3)$ containing S_1, S_2, S_3. A spread $\mathcal{S}$ is called *regular* if the regulus $\mathcal{R}(S_1, S_2, S_3)$ is contained in $\mathcal{S}$ for each three different elements S_1, S_2, S_3 of $\mathcal{S}$. We note that, if $q > 2$, a $(t-1)$-spread of $\mathrm{PG}(2t-1, q)$ is Desarguesian if and only if it is regular [10].

Note that a Desarguesian spread satisfies the property that each subspace spanned by spread elements is partitioned by spread elements (Lemma 2.2 (vii)). Spreads satisfying this property are called *normal* or *geometric*. Clearly, a $(t-1)$-spread in $\mathrm{PG}(2t-1, q)$ is always normal. A $(t-1)$-spread $\mathcal{S}$ in $\mathrm{PG}(rt-1, q)$, with $r > 2$, is normal if and only if $\mathcal{S}$ is Desarguesian [4]. For a survey and self-contained proofs of these characterisations of Desarguesian spreads, we refer to [2].

To explain why the spread $\mathcal{D}_{r,t,q}$ is called 'Desarguesian', we need to consider the following incidence structure constructed from a spread. Let $\mathcal{S}$ be a $(t-1)$-spread in $\mathrm{PG}(rt-1, q)$. Embed $\mathrm{PG}(rt-1, q)$ as a hyperplane H in $\mathrm{PG}(rt, q)$. Consider the following incidence structure $\mathcal{A}(\mathcal{S}) = (\mathcal{P}, \mathcal{L}, \mathrm{I})$, where I is symmetric containment:

$\mathcal{P}$: points of $\mathrm{PG}(rt, q) \setminus H$;

$\mathcal{L}$: t-spaces of $\mathrm{PG}(rt, q)$ intersecting H exactly in an element of $\mathcal{S}$.

Then the incidence structure $\mathcal{A}(\mathcal{S})$ is a $2-(q^{rt}, q^t, 1)$-design with parallelism [4]. These are the same parameters as the parameters of the design obtained from points and lines of an affine space $\mathrm{AG}(r, q^t)$. If $r = 2$, then the $\mathcal{A}(\mathcal{S})$ is an affine translation plane of order q^t, and in this case this construction is known as the *André/Bruck-Bose construction*. The spread $\mathcal{D}_{r,t,q}$ obtained via field reduction is called Desarguesian because the incidence structure $\mathcal{A}(\mathcal{D}_{r,t,q})$ is isomorphic to the design obtained from the points and lines of an affine space $\mathrm{AG}(r, q^t)$. This means that for $r = 2$, the projective completion of the affine plane $\mathcal{A}(\mathcal{S})$ is a Desarguesian projective plane $\cong \mathrm{PG}(2, q^t)$ if and only if the the spread $\mathcal{S}$ is a Desarguesian spread.

Since every linear transformation of $\mathrm{V}(r, q^t)$ can be considered as a linear transformation of $\mathrm{V}(rt, q)$, we have that $\mathrm{GL}(r, q^t) \leq \mathrm{GL}(rt, q)$ (see e.g. [22, p. 139]).

The group of all semilinear transformations of the vector space $\mathrm{V}(r, q^t)$ is denoted by $\Gamma L(r, q^t)$. We show that $\Gamma\mathrm{L}(r, q^t)$ can be embedded in $\Gamma\mathrm{L}(rt, q)$. Any $\sigma \in \mathrm{Aut}(\mathbb{F}_{q^t})$ can be uniquely written as $\tau \circ \rho$, where τ is an element of $\mathrm{Aut}(\mathbb{F}_{q^t})$, fixing $\mathbb{F}_q$ pointwise and ρ is an element of $\mathrm{Aut}(\mathbb{F}_q)$. Now τ induces is an $\mathbb{F}_q$-linear map of $\mathrm{V}(r, q^t)$, so, as seen before, τ can be naturally embedded into $\mathrm{GL}(rt, q)$. Hence, if A is an element of $\mathrm{GL}(r, q^t)$ (hence of $\mathrm{GL}(rt, q)$), then an element ϕ of $\Gamma\mathrm{L}(r, q^t)$ can be written as $A \circ \sigma = A \circ (\tau \circ \rho) = (A \circ \tau) \circ \rho \in \Gamma\mathrm{L}(rt, q)$. It is clear that two different elements of $\Gamma\mathrm{L}(r, q^t)$ correspond to different elements of $\Gamma\mathrm{L}(rt, q)$, so this procedure provides an embedding.

2.2 The Segre variety

In this section we explain the connection between subgeometries and the Segre variety using field reduction. Let us first recall the difference between a subspace and a sub-

geometry. A k-dimensional *subspace* U of $\mathrm{PG}(n,q)$, also called a k-*space*, is isomorphic to a projective space $\mathrm{PG}(k,q)$. A subgeometry B on the other hand is isomorphic to a projective space $\mathrm{PG}(k,q_0)$ for some subfield $\mathbb{F}_{q_0}$ of $\mathbb{F}_q$. We define a *subgeometry* B by the set of points of a projective space $\mathrm{PG}(k,q)$ whose coordinates with respect to some fixed frame take values from a subfield $\mathbb{F}_{q_0}$ of $\mathbb{F}_q$. In this case the subspaces of B correspond to the intersections of subspaces of $\mathrm{PG}(n,q)$ with B. We also say that B is a subgeometry *over* $\mathbb{F}_{q_0}$ or *of order* q_0. For instance, for $k=n$, we take in a projective space $\mathrm{PG}(n,q)$ the set of points B that have coordinates in a subfield $\mathbb{F}_{q_0}$ of $\mathbb{F}_q$, together with all the intersections of subspaces of $\mathrm{PG}(n,q)$ with B. In this way we obtain a subgeometry over $\mathbb{F}_{q_0}$ (*canonical* with respect to the frame to which these coordinates are defined). This subgeometry is isomorphic to a projective space $\mathrm{PG}(n,q_0)$. If $q=q_0^2$, then B is usually called a *Baer subgeometry*.

We have seen in the previous subsection that applying the field reduction map $\mathcal{F}_{r,t,q}$ to all points of a projective space yields a Desarguesian spread $\mathcal{D}_{r,t,q}$. If we apply the field reduction map $\mathcal{F}_{r,t,q}$ to all points of a subgeometry $\mathrm{PG}(r-1,q)$ of $\mathrm{PG}(r-1,q^t)$, then we obtain a subset of $\mathcal{D}_{r,t,q}$ that forms one of the systems of a *Segre variety* $\mathcal{S}_{r-1,t-1}$. We will provide a proof here to give an explicit example of how field reduction works.

Definition 1. The *Segre map* $\sigma_{l,k} : \mathrm{PG}(l,q)\times\mathrm{PG}(k,q)\to\mathrm{PG}((l+1)(k+1)-1,q)$ is defined by

$$\sigma_{l,k}(\mathbb{F}_q(x_0,\ldots,x_l),\mathbb{F}_q(y_0,\ldots,y_k)) := \mathbb{F}_q(x_0y_0,\ldots,x_0y_k,\ldots,x_ly_0,\ldots,x_ly_k).$$

The image of the Segre map $\sigma_{l,k}$ is called the *Segre variety* $\mathcal{S}_{l,k}$.

If we give the points of $\mathrm{PG}((l+1)(k+1)-1,q)$ coordinates in the form

$$\mathbb{F}_q(x_{00},x_{01},\ldots,x_{0k};x_{10},\ldots,x_{1k};\ldots;x_{l0},\ldots,x_{lk}),$$

then it is clear that the points of the Segre variety $\mathcal{S}_{l,k}$ are exactly the points that have coordinates such that the matrix (x_{ij}), $0\le i\le l$, $0\le j\le k$, has rank 1 (see also [19, Theorem 25.5.7]).

By fixing a point in $\mathrm{PG}(l,q)$ and varying the point of $\mathrm{PG}(k,q)$, we obtain a k-dimensional space on $\mathcal{S}_{l,k}$. For every point of $\mathrm{PG}(l,q)$ such a space exists, and the set of these subspaces, which are clearly disjoint, is called a *system* (*of maximal subspaces*). Similarly, by fixing a point in $\mathrm{PG}(k,q)$, we obtain an l-dimensional space on $\mathcal{S}_{l,k}$ by varying the point of $\mathrm{PG}(l,q)$; the set of these subspaces is again called a system (of maximal subspaces). Subspaces of different systems intersect each other in exactly one point, while subspaces within the same system intersect each other trivially. Moreover, each subspace lying on the variety $\mathcal{S}_{l,k}$ is contained in an element of one of these two systems.

Let P be a point of $\mathrm{PG}(r-1,q^t)$, say $P=\mathbb{F}_{q^t}v$, for some nonzero vector $v=(X_0,\ldots,X_{r-1})$, $X_i\in\mathbb{F}_{q^t}$, so P corresponds to the vector line containing the vectors with coordinates $(\lambda_jX_0,\lambda_jX_1,\ldots,\lambda_jX_{r-1})$, where $X_i, i=0,\ldots,r-1$ are fixed elements of $\mathbb{F}_{q^t}$ and λ_j, $j=0,\ldots,q^t-1$ ranges over $\mathbb{F}_{q^t}$.

Now we show that a subgeometry $\Sigma\cong\mathrm{PG}(k-1,q)$ of $\mathrm{PG}(r-1,q^t)$ corresponds to one of the systems of a Segre variety $\mathcal{S}_{k-1,t-1}$ contained in the Segre variety $\mathcal{S}_{r-1,t-1}$.

Theorem 2.4. *If $\mathcal{P}_\Sigma$ is the set of points of a subgeometry $\Sigma\cong\mathrm{PG}(k-1,q)$ of $\mathrm{PG}(r-1,q^t)$ of order q, then $\mathcal{F}_{r,t,q}(\mathcal{P}_\Sigma)$ is projectively equivalent the system of $(t-1)$-spaces of a Segre variety $\mathcal{S}_{k-1,t-1}$ contained in the Segre variety $\mathcal{S}_{r-1,t-1}$.*

Proof. We give a proof for $k = r$, the proof for $k < r$ is easily obtained by replacing $r - k$ coordinates by zero's.

Let ω be a primitive element of $\mathbb{F}_{q^t}$, and consider the $\mathbb{F}_q$-basis $B = \{1, \omega, \omega^2, \ldots, \omega^{t-1}\}$ for $\mathbb{F}_{q^t}$. For every λ_j in $\mathbb{F}_{q^t}$, the element $\lambda_j X_i$ can be expressed in a unique way in terms of this basis, say $\lambda_j X_i = \sum_s x_{is}^j \omega^s$.

This implies that $\mathcal{F}_{r,t,q}(P)$ is the $(t-1)$-dimensional projective space corresponding to the vector space S_v that consists of all vectors

$$v^j := \mathbb{F}_q \left(x_{00}^j, \ldots, x_{0(t-1)}^j; x_{10}^j, \ldots, x_{1(t-1)}^j; \ldots; x_{(r-1)0}^j, \ldots, x_{(r-1)(t-1)}^j \right),$$

with j in $\{0, \ldots, q^t - 1\}$. Assume, without loss of generality, that Σ is canonically embedded in $\mathrm{PG}(r-1, q^t)$ with respect to some fixed frame. It follows from above that applying the field reduction map $\mathcal{F}_{r,t,q}$ to the point P of Σ with coordinates $\mathbb{F}_{q^t}(X_0, \ldots, X_r)$, with $X_i \in \mathbb{F}_q$, gives the $(t-1)$-space of $\mathrm{PG}(rt-1, q)$ spanned by the points

$$\mathbb{F}_q(X_0, 0, \ldots, 0; X_1, 0, \ldots, 0; \ldots; X_{r-1}, 0, \ldots, 0),$$

$$\mathbb{F}_q(0, X_0, \ldots, 0; 0, X_1, \ldots, 0; \ldots; 0, X_{r-1}, \ldots, 0),$$

$$\mathbb{F}_q(0, \ldots 0, X_0; 0, \ldots, 0, X_1; \ldots; 0, \ldots, 0, X_{r-1}).$$

Hence $\mathcal{F}_{r,t,q}(P)$ contains the points with coordinates

$$\mathbb{F}_q(\mu_0 X_0, \mu_1 X_0, \ldots, \mu_{t-1} X_0; \mu_0 X_1, \ldots, \mu_{t-1} X_1; \ldots; \mu_0 X_{r-1}, \ldots, \mu_{t-1} X_{r-1}),$$

$\mu_0, \ldots, \mu_{t-1} \in \mathbb{F}_q$. Since the matrix (x_{ij}) with $x_{ij} = \mu_i X_j$, corresponding to these coordinates has rank 1, the points of $\mathcal{F}_{r,t,q}(P)$ lie on the Segre variety $\mathcal{S}_{r-1,t-1}$. □

Corollary 2.5. *The system of $(t-1)$-spaces of a Segre variety $\mathcal{S}_{k-1,t-1}$ in $\mathrm{PG}(rt-1, q)$, $k \leq r$, is projectively equivalent to a subset of $\mathcal{D}_{r,t,q}$, whereas the system of $(r-1)$-spaces of a Segre variety $\mathcal{S}_{r-1,u-1}$ in $\mathrm{PG}(rt-1, q)$, $u \leq t$, is projectively equivalent to a subset of $\mathcal{D}_{t,r,q}$.*

3 Field reduction for classical polar spaces

In this section we elaborate on the concept of field reduction for classical polar spaces; starting from a classical polar space in $\mathrm{PG}(r-1, q^t)$ we want to obtain a classical polar space in $\mathrm{PG}(rt-1, q)$. We will see that field reduction for classical polar spaces is somewhat more involved than field reduction for projective spaces. The reason is the extra freedom that arises from the choice of the form that is used to obtain a polar space in $\mathrm{PG}(rt-1, q)$; different forms can give different types of polar spaces in $\mathrm{PG}(rt-1, q)$.

Polar spaces are incidence structures that can be defined axiomatically, see [53], but here we only need the so-called *classical polar spaces*, i.e. polar spaces that are embedded in a projective space equipped with an appropriate sesquilinear form. A celebrated result of Tits [50] shows that every finite polar space of rank at least 3 is *classical*.

3.1 Classical polar spaces

Let $Q(X_0, \ldots, X_n) = \sum_{i,j=0, i \leq j}^{n} a_{ij} X_i X_j$ be a quadratic form over $\mathbb{F}_q$. A *quadric* $\mathcal{Q}$ in $\mathrm{PG}(n,q)$ is the set of points $\mathbb{F}_q v$ that satisfy $Q(v) = 0$. Let q be a square and let $H(X_0, \ldots, X_n) = \sum_{i,j=0}^{n} a_{ij} X_i X_j^{\sqrt{q}}$ with $a_{ij} = a_{ji}^{\sqrt{q}}$, be a Hermitian form over $\mathbb{F}_q$. A *Hermitian variety* in $\mathrm{PG}(n,q)$, denoted by $\mathcal{H}(n,q)$, is the set of points $\mathbb{F}_q v$ that satisfy $H(v) = 0$. A quadric or Hermitian variety of $\mathrm{PG}(n,q)$ is called *singular* if there exists a coordinate transformation which reduces the form to one in fewer variables, otherwise, the quadric or Hermitian variety is called *non-singular*.

If n is even, all non-singular quadrics in $\mathrm{PG}(n,q)$ are projectively equivalent to the quadric with equation $X_0^2 + X_1 X_2 + \ldots + X_{n-1} X_n = 0$. These quadrics are called *parabolic* and are denoted by $\mathcal{Q}(n,q)$.

If n is odd, a non-singular quadric in $\mathrm{PG}(n,q)$ is either projectively equivalent to the quadric with equation $X_0 X_1 + \ldots + X_{n-1} X_n = 0$ or to the quadric with equation $f(X_0, X_1) + X_2 X_3 + \ldots + X_{n-1} X_n = 0$, where f is an irreducible homogeneous quadratic form over $\mathbb{F}_q$. Quadrics of the first type are called *hyperbolic* and are denoted by $\mathcal{Q}^+(n,q)$, quadrics of the second type are called *elliptic* and are denoted by $\mathcal{Q}^-(n,q)$.

The incidence structure defined by a nonsingular quadratic or Hermitian variety, consisting of the subspaces that are contained in the variety all form polar spaces. We use the same notation for the polar space and the varieties. The polar spaces $\mathcal{Q}(n,q)$, $\mathcal{Q}^+(n,q)$, and $\mathcal{Q}^-(n,q)$ are called the *orthogonal polar spaces*, respectively of *parabolic*, *hyperbolic* and *elliptic* type; the polar space $\mathcal{H}(n,q)$ is called the *Hermitian* or *unitary polar space*.

Examples of quadrics and Hermitian varieties can be constructed using a *polarity*, which is a collineation of order two, of $\mathrm{PG}(n,q)$ onto its dual space. The image of a subspace π under a polarity is denoted by $\pi^\perp$ and is called the *polar (space) of* π. If a subspace π is contained in $\pi^\perp$, then π is called *absolute*. A polarity is determined by a field automorphism σ and a non-singular matrix A. There are four types of polarities (σ, A) of $\mathrm{PG}(n,q)$, listed below.

(i) If $\sigma = 1$, q odd, $A = A^T$, then the polarity (σ, A) is called an *orthogonal* polarity.

(ii) If $\sigma = 1$, $A = -A^T$, and $a_{ii} = 0$ for all i, then every point is an absolute point, n should be odd, and the polarity (σ, A) is called a *symplectic* polarity.

(iii) If $\sigma = 1$, q even, $A = A^T$ and $a_{ii} \neq 0$ for some i, then the polarity (σ, A) is called a *pseudo-polarity*.

(iv) If $\sigma \neq 1$, then q is a square, $\sigma : x \mapsto x^{\sqrt{q}}$, $A = A^{T\sigma}$ and (σ, A) is called a *Hermitian* or *unitary* polarity.

If q is odd, then the absolute points of an orthogonal polarity form a quadric in $\mathrm{PG}(n,q)$. If q is a square, then the absolute points of a Hermitian polarity form a Hermitian variety in $\mathrm{PG}(n,q)$.

The points of $\mathrm{PG}(n,q)$, n odd, $n \geq 3$, together with the absolute subspaces of a symplectic polarity of $\mathrm{PG}(n,q)$ form a *symplectic polar space*, denoted by $\mathcal{W}(n,q)$.

Together the polar spaces $\mathcal{Q}(n,q)$, $\mathcal{Q}^+(n,q)$, $\mathcal{Q}^-(n,q)$, $\mathcal{H}(n,q)$ and $\mathcal{W}(n,q)$ are called the *classical polar spaces*. If r is the maximum dimension of a subspace contained in a classical polar space $\mathcal{P}$, then $r+1$ is the *rank* of $\mathcal{P}$.

The classical polar spaces can also be introduced using the theory of sesquilinear forms on $\mathbb{F}_q^n$. If Q denotes the quadratic form defining one of the orthogonal polar spaces, then the associated bilinear form $\beta_Q(x,y) := Q(x+y) - Q(x) - Q(y)$ is symmetric, and if q is odd, the quadratic form can be obtained from the bilinear form. Similarly $\mathcal{H}(n,q)$ corresponds to a σ-sesquilinear form $\beta_{\mathcal{H}}$, where $x^\sigma = x^{\sqrt{q}}$ (called *unitary form*), and $\mathcal{W}(n,q)$ corresponds to an alternating bilinear form $\beta_{\mathcal{W}}$. Note that if β is a form corresponding to one of the classical polar spaces, and $\pi \mapsto \pi^\perp$ is the associated polarity, then we have $\beta(x,y) = 0$ if and only if the hyperplane $(\mathbb{F}_q x)^\perp$ contains the point $\mathbb{F}_q y$. We call a subspace π *totally isotropic* with respect to the form β if for all points $\mathbb{F}_q x$ and $\mathbb{F}_q y$ in π, $\beta(x,y) = 0$. A symmetric bilinear form with $\beta(x,x) \neq 0$ for some x is called a *pseudo-symplectic*.

Let $\mathcal{P}$ be one of the orthogonal polar spaces in $\mathrm{PG}(n,q)$ with associated quadratic form Q and bilinear form β_Q. A *hyperbolic line* of $\mathcal{P}$ is a line containing two points $\mathbb{F}_q x$ and $\mathbb{F}_q y$ with $Q(x) = Q(y) = 0$ and $\beta_Q(x,y) = 1$.

The classification of quadratic forms over finite fields then gives us the following.

- The polar space $\mathcal{Q}^+(2n+1,q)$ is the orthogonal sum of $n+1$ hyperbolic lines.
- The polar space $\mathcal{Q}^-(2n+1,q)$ is the orthogonal sum of n hyperbolic lines and an *elliptic line*, corresponding to $f(X_0, X_1)$.
- The polar space $\mathcal{Q}(2n,q)$ is the orthogonal sum of n hyperbolic lines and a point $\mathbb{F}_q x_0$ with $Q(x_0) \neq 0$, and we define the *sign of a parabolic quadric* $\mathcal{Q}(2n,q)$ to be $+1$ if $Q(x_0)$ is a square in $\mathbb{F}_q$ and -1 otherwise.

The classical polar spaces as described above correspond to the classical groups: the orthogonal groups $O^+(2n,q)$, $O^-(2n,q)$, and $O(2n+1,q)$, the unitary group $U(n,q)$, and the symplectic group $Sp(n,q)$. The correspondence between the forms, the polar spaces, and the groups is given in the following table.

Quadratic form	Polar space	Associated group
hyperbolic	$\mathcal{Q}^+(2n-1,q)$	$O^+(2n,q)$
elliptic	$\mathcal{Q}^-(2n-1,q)$	$O^-(2n,q)$
parabolic	$\mathcal{Q}(2n,q)$	$O(2n+1,q)$
Bilinear form	Polar space	Associated group
hermitian	$\mathcal{H}(n-1,q)$	$U(n,q)$
alternating	$\mathcal{W}(n-1,q)$	$Sp(n,q)$

3.2 Field reduction and forms

In order to obtain a polar space in $\mathrm{PG}(rt-1,q)$ from a polar space in $\mathrm{PG}(r-1,q^t)$, we associate a form on $\mathbb{F}_q^{rt}$ starting from a form on $\mathbb{F}_{q^t}^r$ using the trace map. Let Tr denote the *trace map* from $\mathbb{F}_{q^t}$ to $\mathbb{F}_q$,

$$Tr = Tr_{\mathbb{F}_{q^t}/\mathbb{F}_q} : \mathbb{F}_{q^t} \mapsto \mathbb{F}_q : x \to x + x^q + \ldots + x^{q^{t-1}}.$$

Let f be a form on $\mathbb{F}_{q^t}^r$, and let L_α be the map $\mathbb{F}_{q^t} \mapsto \mathbb{F}_q : x \to Tr(\alpha x)$ with $\alpha \in \mathbb{F}_{q^t}$. The map $L_\alpha f = L_\alpha \circ f$ is clearly a form on $\mathbb{F}_q^{rt}$. If f and $L_\alpha f$ are non-degenerate, then

starting from a polar space in $\mathrm{PG}(r-1,q^t)$ with corresponding quadratic, alternating or hermitian form on $\mathbb{F}_{q^t}^r$, by *field reduction*, we can obtain a polar space in $\mathrm{PG}(rt-1,q)$.

In [16], N. Gill determines the conditions on f and α to ensure that $L_\alpha f$ is non-degenerate if f is non-degenerate.

Theorem 3.1. *[16, Theorem A] Let β be a reflexive σ-sesquilinear form on $V(r,q^t)$, Q a quadratic form, and $L_\alpha : \mathbb{F}_{q^t} \to \mathbb{F}_q : x \mapsto Tr(\alpha x)$. Then*
(i) $L_\alpha\beta$ is non-degenerate if and only if β is non-degenerate and $\alpha \neq 0$;
(ii) if q is even and r is odd, then $L_\alpha Q$ is degenerate;
(iii) if q is odd or r is even, then $L_\alpha Q$ is non-degenerate if and only if Q is non-degenerate and $\alpha \neq 0$.

Lemma 3.2. *Let $L_\alpha : \mathbb{F}_{q^t} \to \mathbb{F}_q : x \mapsto Tr(\alpha x)$, $\alpha \in \mathbb{F}_{q^t}^*$. Suppose that $L_\alpha\beta$ and $L_\alpha Q$ are non-degenerate. The image under the field reduction map of an absolute subspace of a polar space in $\mathrm{PG}(r-1,q^t)$, with associated sesquilinear form β or quadratic form Q, is an absolute subspace in $\mathrm{PG}(rt-1,q)$ of the polar space with associated sesquilinear form $L_\alpha\beta$ or quadratic form $L_\alpha Q$.*

Proof. Suppose π is an absolute subspace of the polar space in $\mathrm{PG}(r-1,q^t)$ with associated sesquilinear form β. Then for each two points $\mathbb{F}_{q^t}x, \mathbb{F}_{q^t}y$ in π we have $\beta(\lambda x, \mu y) = 0$, $\forall \lambda, \mu \in \mathbb{F}_{q^t}$, and hence $L_\alpha\beta(\lambda x, \mu y) = 0$, $\forall \lambda, \mu \in \mathbb{F}_{q^t}$. This implies that for each two points $\mathbb{F}_q u$ and $\mathbb{F}_q v$ in $\mathcal{F}_{r,t,q}(\pi)$ we have $L_\alpha\beta(u,v) = 0$. It follows that $\mathcal{F}_{r,t,q}(\pi)$ is absolute with respect to $L_\alpha\beta$. The proof is analogous using a quadratic form. □

3.2.1 Quadratic form field reduction

The orthogonal polar spaces are defined by a quadratic form, and the field reduction of these spaces is studied using that form.

In [16] the author determines the possible polar spaces that can be obtained for each quadratic form. The approach used in [16] is from a group theory perspective, so we will go through the list of possibilities, and give elementary proofs of the results using our terminology. We obtain slightly different conditions.

Field reduction does not change the type of the orthogonal polar spaces in odd dimensional projective space. For the orthogonal polar space in even dimensional projective space, i.e. of parabolic type, the situation is more complicated.

Theorem 3.3. *Let Q be a non-degenerate quadratic form on $\mathbb{F}_{q^t}^r$ corresponding to the polar space $\mathcal{Q}$, and let $L_\alpha : \mathbb{F}_{q^t} \to \mathbb{F}_q : x \mapsto Tr(\alpha x)$, $\alpha \in \mathbb{F}_{q^t}^*$. Suppose $L_\alpha Q$ is non-degenerate and let $\mathcal{Q}'$ denote the polar space defined by $L_\alpha Q$. Then the following holds:*
(i) if $\mathcal{Q}$ is of hyperbolic type, then so is $\mathcal{Q}'$;
(ii) if $\mathcal{Q}$ is of elliptic type, then so is $\mathcal{Q}'$;
(iii) if $\mathcal{Q}$ is of parabolic type, choose $\gamma \in \mathbb{F}_{q^t}^*$ a square if $sign(\mathcal{Q}) = 1$ and a non-square if $sign(\mathcal{Q}) = -1$, then q is odd and

- *$\mathcal{Q}'$ is of parabolic type if t is odd;*
- *if t is even then $\mathcal{Q}'$ is of hyperbolic type if (a) $q^{t/2} \equiv 1 \bmod 4$, and $\alpha\gamma$ is a non-square in $\mathbb{F}_{q^t}$ or (b) $q^{t/2} \equiv 3 \bmod 4$, and $\alpha\gamma$ is a square in $\mathbb{F}_{q^t}$;*

- *$\mathcal{Q}'$ is of elliptic type in the remaining cases.*

Proof. (i) Since $\mathcal{Q}$ has rank $r/2$, the polar space $\mathcal{Q}'$ will have rank at least $rt/2$, by Lemma 3.2. This implies that $\mathcal{Q}'$ is of hyperbolic type.

(ii) If $\mathcal{Q}$ is of elliptic type, then r is even, say $r = 2n$, and we know that up to the choice of a basis it is the orthogonal sum of a $Q^-(1, q^t)$ and $n-1$ hyperbolic lines. The additivity of L_α and part (i) imply that $L_\alpha Q$ is the orthogonal sum of the field reduced $Q^-(1, q^t)$ and $n-1$ copies of a $(2t-1)$-dimensional space of hyperbolic type.

So we only need to consider $L_\alpha Q$ with Q of elliptic type in $\mathrm{PG}(1, q^t)$. If $L_\alpha Q$ is of hyperbolic type, then w.l.o.g. we may assume that the $(t-1)$-space $\pi = \{\langle (y, g(y))\rangle_{\mathbb{F}_q} : y \in \mathbb{F}_{q^t}^*\}$, with $g(Y) = \sum_{j=0}^{t-1} g_j Y^{q^j}$ some $\mathbb{F}_q$-linear map, is totally isotropic with respect to $L_\alpha Q$, where $Q(X_0, X_1) = aX_0^2 + bX_0X_1 + cX_1^2$ irreducible in $\mathbb{F}_{q^t}[X_0, X_1]$. This means that

$$Tr(\alpha(ay^2 + byg(y) + cg(y)^2)) = 0 \text{ for all } y \in \mathbb{F}_{q^t}. \tag{3}$$

But $Tr(\alpha(aY^2 + bYg(Y) + cg(Y)^2))$ reduces, modulo $Y^{q^t} - Y$, to a polynomial of degree $\leq 2q^{t-1}$ in Y which is less than q^t if $q > 2$. So if $q > 2$, this implies that $Q(X_0, X_1)$ is reducible, which is a contradiction, and we may conclude that there is no totally isotropic $(t-1)$-space. Therefore $L_\alpha Q$ and hence $\mathcal{Q}'$ is of elliptic type. If $q = 2$ then using $Tr(\gamma y^2) = Tr((\gamma)^{1/2} y)$, the polynomial $Tr(\alpha(aY^2 + bYg(Y) + cg(Y)^2))$ reduces, modulo $Y^{2^t} - Y$, to a polynomial of degree $\leq 2^{t-1}$ in Y which less than 2^t, and hence again equation (3) implies that $aY^2 + bYg(Y) + cg(Y)^2$ is reducible. We may conclude that also for $q = 2$ the polar space $\mathcal{Q}'$ is of elliptic type.

(iii) Suppose $\mathcal{Q}$ is of parabolic type. By the non-degeneracy hypothesis this implies that q is odd. If t is odd, then rt is odd and $L_\alpha Q$ must be of parabolic type. Next we consider the case when t is even.

W.l.o.g. assume that $\mathcal{Q}$ is the orthogonal sum of $(r-1)/2$ hyperbolic lines and the point $\mathbb{F}_{q^t} x_0$, where $Q(x_0) = \gamma \neq 0$. Again, as in part (ii), using the additivity of L_α and part (i) imply that we only need to consider $L_\alpha Q$ with $Q(X_0) = \gamma X_0^2$. Note that $L_\alpha Q$ is of hyperbolic type if and only if $\exists u \in \mathbb{F}_{q^t}^*$ such that $Tr(\alpha\gamma u^2) = 0$, otherwise $L_\alpha Q$ is of elliptic type.

First suppose that $t = 2$. We have

$$Tr(\alpha\gamma u^2) = 0 \;\Leftrightarrow\; \alpha\gamma u^2(1 + (\alpha\gamma u^2)^{q-1}) = 0 \;\Leftrightarrow\; (\alpha\gamma u^2)^{q-1} = -1.$$

If ω is a primitive element of $\mathbb{F}_{q^2}$, then this is equivalent to

$$(\alpha\gamma u^2)^{q-1} = \omega^{(q^2-1)/2} \;\Leftrightarrow\; u^2 = \frac{\xi\omega^{(q+1)/2}}{\alpha\gamma},$$

for some $\xi \in \mathbb{F}_q^*$. We have shown that $L_\alpha Q$ is of hyperbolic type if and only if $\exists u \in \mathbb{F}_{q^2}^*$ such that $u^2 = \frac{\xi\omega^{(q+1)/2}}{\alpha\gamma}$, for some $\xi \in \mathbb{F}_q^*$. Note that ξ is a square in $\mathbb{F}_{q^2}$ and $\omega^{(q+1)/2}$ is a square in $\mathbb{F}_{q^2}$ if and only if $q = 3 \bmod 4$. This gives us the following conditions: $L_\alpha Q$ is of hyperbolic type if and only if

(a") $q \equiv 1 \bmod 4$ and $\alpha\gamma$ is a non-square in $\mathbb{F}_{q^2}$;

(b") $q \equiv 3 \bmod 4$ and $\alpha\gamma$ is a square in $\mathbb{F}_{q^2}$.

Next suppose $t > 2$ even. If $t' = t/2$ then $\mathbb{F}_q \subset \mathbb{F}_{q^{t'}} \subset \mathbb{F}_{q^t}$ and

$$Tr = Tr_{\mathbb{F}_{q^t}/\mathbb{F}_q} = Tr_{\mathbb{F}_{q^{t'}}/\mathbb{F}_q} Tr_{\mathbb{F}_{q^t}/\mathbb{F}_{q^{t'}}}.$$

Applying parts (i) and (ii) and the arguments used for the case $t = 2$, the conditions (a") and (b") become

(a') $q^{t/2} \equiv 1 \bmod 4$ and $\alpha\gamma$ is a non-square in $\mathbb{F}_{q^t}$;

(b') $q^{t/2} \equiv 3 \bmod 4$ and $\alpha\gamma$ is a square in $\mathbb{F}_{q^t}$.

Using the fact that γ is a square if and only if $sign(\mathcal{Q}) = 1$ concludes the proof. □

3.2.2 Bilinear form field reduction

For the Hermitian and symplectic polar spaces, we need to use the sesquilinear form to study the possible polar spaces that are obtained after field reduction. The following theorem, from [16], summarises the results, where *atypical* indicates that the bilinear form is not of one of the prescribed types.

Theorem 3.4. *[16, Theorem C] Let β be a non-degerate σ-sesquilinear form $\beta : \mathbb{F}_{q^t}^r \times \mathbb{F}_{q^t}^r \to \mathbb{F}_{q^t}$, with corresponding polar space of hermitian or symplectic type, and $L_\alpha = Tr \circ \alpha$ with $0 \neq \alpha \in \mathbb{F}_{q^t}$. Then the type of $L_\alpha\beta$ is as follows.*

Type of β	*Type of $L_\alpha\beta$*	*Conditions*	*Embedding*
hermitian	*hermitian*	*t odd, $\sigma(\alpha) = \alpha$*	$U(r, q^t) \leq U(rt, q)$
hermitian	*atypical*	*t odd, $\sigma(\alpha) \neq \alpha$*	–
hermitian	*alternating*	*t even, q even, $\sigma(\alpha) = \alpha$*	$U(r, q^t) \leq Sp(rt, q)$
hermitian	*alternating*	*t even, q odd, $\sigma(\alpha) = -\alpha$*	$U(r, q^t) \leq Sp(rt, q)$
hermitian	*atypical*	*t even, $\sigma(\alpha) \neq \pm\alpha$*	–
hermitian	*hyperbolic*	*t even, q odd, r even, $\sigma(\alpha) = \alpha$*	$U(r, q^t) \leq O^+(rt, q)$
hermitian	*elliptic*	*t even, q odd, r odd, $\sigma(\alpha) = \alpha$*	$U(r, q^t) \leq O^-(rt, q)$
alternating	*alternating*	–	$Sp(r, q^t) \leq Sp(rt, q)$
pseudo-symplectic	*pseudo-symplectic*	*q even*	–

The last column of the table provides a list of possible embeddings in terms of the associated groups.

3.2.3 Conclusion

We summarise the possibilities for field reduction of the classical polar spaces in the following table, where the polar space in $\mathrm{PG}(rt - 1, q)$ is obtained from the polar space in $\mathrm{PG}(r - 1, q^t)$ using the map $L_\alpha : \mathbb{F}_{q^t} \to \mathbb{F}_q \ : \ x \mapsto Tr_{\mathbb{F}_{q^t}/\mathbb{F}_q}(\alpha x)$ with $\alpha \in \mathbb{F}_{q^t}^*$.

Polar space in $\mathrm{PG}(r-1,q^t)$	Polar space in $\mathrm{PG}(rt-1,q)$	Conditions r, t, q	Conditions $\alpha \neq 0$
hyperbolic	*hyperbolic*	*r even*	–
elliptic	*elliptic*	*r even*	–
parabolic	*parabolic*	*r odd*, *t odd*, *q odd*	–
parabolic	*hyperbolic or elliptic*	*r odd*, *t even*	$(*)$
hermitian	*hermitian*	*t odd*, *q square*	$\sigma(\alpha)=\alpha$
hermitian	*symplectic*	*t even*	$\sigma(\alpha)=-\alpha$
hermitian	*hyperbolic*	*t even*, *q odd*, *r even*	$\sigma(\alpha)=\alpha$
hermitian	*elliptic*	*t even*, *q odd*, *r odd*	$\sigma(\alpha)=\alpha$
symplectic	*symplectic*	*r even*	–

$(*)$ hyperbolic if ($q^{t/2}=1 \mod 4$ and $\alpha\gamma \notin \square$) or ($q^{t/2}=3 \mod 4$ and $\alpha\gamma \in \square$); elliptic in the remaining cases, where $\square$ denotes the set of non-zero squares in $\mathbb{F}_{q^t}$ and $\gamma \in \square$ if $sign(\mathcal{Q})=1$ and $\gamma \in \mathbb{F}_{q^t}^* \setminus \square$ if $sign(\mathcal{Q})=-1$.

Field reduction for polar spaces (also called the 'trace trick') was used already in 1994 by Shult and Thas [43] to construct m-systems of polar spaces. Later on, the theory of *intriguing sets* extended that of m-systems and Kelly [21] used field reduction to construct new examples of intriguing sets of polar spaces.

4 Linear sets in projective spaces

Linear sets generalise the concept of subgeometries in a projective space. They have many applications in finite geometry; linear sets have been intensively used in recent years in order to classify, construct or characterise various geometric structures, e.g. blocking sets and semifields that will be discussed at the end of this paper. For a further discussion of these and other applications, we refer to the survey of O. Polverino [41].

4.1 Definition

To obtain a linear set in a projective space, some kind of reverse field reduction is used. The field reduction map takes as input a subspace of $\mathrm{PG}(r-1,q^t)$ and returns a subspace of $\mathrm{PG}(rt-1,q)$. Or in other words from an $\mathbb{F}_{q^t}$-subspace we obtain an $\mathbb{F}_q$-subspace. A linear set, on the other hand, is defined by an $\mathbb{F}_q$-subspace and returns, not a subspace, but a subset of a projective $\mathbb{F}_{q^t}$-linear space, i.e. a subset of some $\mathrm{PG}(r-1,q^t)$.

More precisely, let $V=\mathbb{F}_{q^t}^r$. A set L of points in $\mathrm{PG}(V)$ is called an $\mathbb{F}_q$-*linear set* (*of rank* k) if there exists a subset U of V that forms a (k-dimensional) $\mathbb{F}_q$-subspace of V, such that $L=\mathcal{B}(U)$, where

$$\mathcal{B}(U) := \{\mathbb{F}_{q^t}u : \ u \in U \setminus \{0\}\}.$$

Often the notation L_U is used to indicate the underlying subspace. Obviously, if we say that the subset U forms an $\mathbb{F}_q$-subspace of V, then we mean a subspace of the rt-dimensional space that is obtained by considering V as vector space over $\mathbb{F}_q$. But from now on, we identify the $\mathbb{F}_q$-vector subspace U with the subset U. This allows us to consider the projective subspace $\mathrm{PG}(U)$ in $\mathrm{PG}(rt-1,q)$. We summarize the above in

the following diagram

$$\begin{array}{ccccccc} U & \subseteq & \mathbb{F}_{q^t}^r & \longleftrightarrow & \mathbb{F}_q^{rt} & \supseteq & U \\ & & \updownarrow & & \updownarrow & & \updownarrow \\ L_U = \mathcal{B}(U) & \subseteq & \mathrm{PG}(r-1,q^t) & \longleftrightarrow & \mathrm{PG}(rt-1,q) & \supseteq & \mathrm{PG}(U) \end{array}$$

Recall that the field reduction map $\mathcal{F}_{r,t,q}$ gives us a one-to-one correspondence between the points of $\mathrm{PG}(r-1,q^t)$ and the elements of a Desarguesian spread $\mathcal{D}_{r,t,q}$. This gives us a more geometric perspective on the notion of a linear set; namely, an $\mathbb{F}_q$-linear set is a set L of points of $\mathrm{PG}(r-1,q^t)$ for which there exists a subspace π in $\mathrm{PG}(rt-1,q)$ such that the points of L correspond to the elements of $\mathcal{D}_{r,t,q}$ that have a non-empty intersection with π. If there is no confusion possible, we will often identify the elements of $\mathcal{D}_{r,t,q}$ with the points of $\mathrm{PG}(r-1,q^t)$, i.e. a point P is identified with its image under $\mathcal{F}_{r,t,q}$. This allows us to view $\mathcal{B}(\pi)$ as a subset of $\mathcal{D}_{r,t,q}$. This is illustrated by the following diagram, where as before $\mathcal{P}$ denotes the set of points of $\mathrm{PG}(r-1,q^t)$.

$$\begin{array}{ccccccc} & & \mathrm{PG}(r-1,q^t) & \longleftrightarrow & \mathrm{PG}(rt-1,q) & \supseteq & \pi \\ & & \downarrow & & \downarrow & & \Downarrow \\ L = \mathcal{B}(\pi) & \subseteq & \mathcal{P} & \overset{\mathcal{F}_{r,t,q}}{\longleftrightarrow} & \mathcal{D} & \supseteq & \mathcal{B}(\pi) \end{array}$$

If P is a point of $\mathcal{B}(\pi)$ in $\mathrm{PG}(r-1,q^t)$, where π is a subspace of $\mathrm{PG}(rt-1,q)$, then we define the *weight of* P as $wt(P) := \dim(\mathcal{F}_{r,t,q}(P) \cap \pi) + 1$. This makes a point to have weight 1 if its corresponding spread element intersects π in a point. It is clear that a point of an $\mathbb{F}_q$-linear set of rank k in $\mathrm{PG}(r-1,q^t)$ can have weight at most $\min\{k,t\}$.

Theorem 4.1. *Let $S = \mathcal{B}(\pi)$ be a linear set of rank $k > 0$ and denote by x_i the number of points of weight i, with $m = \min\{k,t\}$, then the following relations hold:*
(i) $|S| = x_1 + x_2 + \cdots + x_m$
(ii) $x_1 + (q+1)x_2 + \frac{q^3-1}{q-1}x_3 + \cdots + \frac{q^m-1}{q-1}x_m = \frac{q^k-1}{q-1}$
(iii) $|S| \leq \frac{q^k-1}{q-1}$
(iv) $|S| \equiv 1 \mod q$.

Proof. For (ii), count the couples $\{(P \in \pi, \mathcal{B}(P))\}$, the other items follow directly. □

If π intersects the elements of $\mathcal{D}$ in at most a point, i.e. the size of $\mathcal{B}(\pi)$ is maximal, or equivalently every point of $\mathcal{B}(\pi)$ has weight one, then we say that π is *scattered with respect to* $\mathcal{D}$; in this case $\mathcal{B}(\pi)$ is called a *scattered linear set*. The notion of scattered linear sets was introduced in [7], where the following bound on the rank of a scattered linear set was obtained.

Theorem 4.2. *[7, Theorem 4.3] A scattered $\mathbb{F}_q$-linear set in $\mathrm{PG}(r-1,q^t)$ has rank $\leq rt/2$.*

Scattered linear sets that meet this bound are called *maximum scattered*. Maximum linear sets are related to interesting geometric objects such as two-weight codes, two-intersection sets and strongly regular graphs (see [23]). The connection with pseudoreguli will be explained in Section 4.5, and the for the connection with particular classes of semifields (see Section 6) we refer to [37] and more recent [26].

We have the following useful lemma for linear sets.

Lemma 4.3. *Let $\mathcal{D}$ be the Desarguesian $(t-1)$-spread of $\mathrm{PG}(rt-1,q)$. Let $\mathcal{B}(\pi)$ be a linear set of rank $k+1$, where π is a k-dimensional space. For every point R in $\mathrm{PG}(rt-1,q)$, contained in an element of $\mathcal{B}(\pi)$, there is a k-dimensional space π', through R, such that $\mathcal{B}(\pi)=\mathcal{B}(\pi')$.*

Proof. Since all Desarguesian spreads are equivalent, we may assume $\mathcal{D}=\mathcal{D}_{r,t,q}$, the image of the set of points of $\mathrm{PG}(r-1,q^t)$ under the field reduction map $\mathcal{F}_{r,t,q}$. Let φ_ω, for $\omega\neq 0$, be the collineation of $\mathrm{PG}(rt-1,q)$ mapping a point $\mathbb{F}_q x$ of $\mathrm{PG}(rt-1,q)$ to $\mathbb{F}_q \omega x$. Then φ_ω fixes each element of $\mathcal{D}_{r,t,q}$ since $\mathbb{F}_{q^t}x=\mathbb{F}_{q^t}\omega x$. Moreover, the set

$$\{\mathbb{F}_q\omega x \ : \ \omega\in\mathbb{F}_{q^t}\setminus\{0\}\}$$

consists of the $(q^t-1)/(q-1)$ different points of $\mathcal{B}(\mathbb{F}_q x)$.

Let R be a point contained in an element $\mathcal{F}_{r,t,q}(P)$ of $\mathcal{B}(\pi)$, and let T be a point in $\pi\cap\mathcal{F}_{r,t,q}(P)$. It follows from the previous part that $R=T^{\varphi_\omega}$ for some $\omega\in\mathbb{F}_{q^t}$.

If $\mathbb{F}_q z\in\pi$, then $(\mathbb{F}_q z)^{\varphi_\omega}=\mathbb{F}_q\omega z\in\mathcal{B}(\mathbb{F}_q z)\in\mathcal{B}(\pi)$, and hence $\mathcal{B}(\pi^{\varphi_\omega})\subset\mathcal{B}(\pi)$. Since φ_ω is a collineation $\mathcal{B}(\pi^{\varphi_\omega})=\mathcal{B}(\pi)$. □

From this lemma, we have for every point R in $\mathrm{PG}(rt-1,q)$, contained in an element of $\mathcal{B}(\pi)$, where π is $(k-1)$-dimensional, there is a $(k-1)$-dimensional space π', through R, such that $\mathcal{B}(\pi)=\mathcal{B}(\pi')$. This raises an important question: how many different subspaces π' of dimension $(k-1)$ are there through a fixed point R such that $\mathcal{B}(\pi')=\mathcal{B}(\pi)$? If $\mathcal{B}(\pi)$ is a regulus, this means π is a line, then it is clear that through every point of an element of $\mathcal{B}(\pi)$, there is exactly one line π' such that $\mathcal{B}(\pi')=\mathcal{B}(\pi)$, because through every point of a regulus, there exists a unique transversal line to this regulus. In Theorem 4.8 we will see that the answer to this question is not always equal to one. Some cases are well understood, but in general, this question remains open.

4.2 Linear sets and projections of subgeometries

It is clear from the definition (or from the link with Segre varieties described in Section 2.2) that a subgeometry is a linear set, but a linear set is not necessarily a subgeometry. However, the following theorem by Lunardon and Polverino shows that every linear set is a projection of a subgeometry. For the particular case of linear *blocking sets*, this was proven in [39], for the case of scattered linear sets, but not using this terminology, it was shown already in 1981 in [32].

Let $\Sigma=\mathrm{PG}(k-1,q)$ be a subgeometry of $\Sigma^*=\mathrm{PG}(k-1,q^t)$ and suppose there exists an $(k-r-1)$-dimensional subspace Ω^* of Σ^* disjoint from Σ. Let $\Omega=\mathrm{PG}(r-1,q^t)$ be an $(r-1)$-dimensional subspace of Σ^* disjoint from Ω^*. Let $p_{\Omega^*,\Omega}$ denote the projection map defined by $x\mapsto\langle\Omega^*,x\rangle\cap\Omega$ for each point $x\in\Sigma^*\setminus\Omega^*$. The point set $\Gamma=p_{\Omega^*,\Omega}(\Sigma)$, i.e., the image of Σ under the projection map $p_{\Omega^*,\Omega}$ is simply called the *projection* of Σ from Ω^* into Ω.

Theorem 4.4. *[36, Theorem 1 and 2] If Γ is a projection of $\mathrm{PG}(k-1,q)$ into $\Omega = \mathrm{PG}(r-1,q^t)$ with $k \geq r$, then Γ is an $\mathbb{F}_q$-linear set of rank k and $\langle \Gamma \rangle = \Omega$. Conversely, if L is an $\mathbb{F}_q$-linear set of Ω of rank k and $\langle L \rangle = \Omega = \mathrm{PG}(r-1,q^t)$, then either L is a canonical subgeometry of Ω or there are a $(k-r-1)$-dimensional subspace Ω^* of $\Sigma^* = \mathrm{PG}(k-1,q^t)$ disjoint from Ω and a canonical subgeometry Σ of Σ^* disjoint from Ω^* such that $L = p_{\Omega^*,\Omega}(\Sigma)$.*

Corollary 4.5. *The set $\mathcal{B}(\pi)$ of elements of $\mathcal{D}_{r,t,q}$, where π is a $(k-1)$-dimensional space in $\overline{\Omega} = \mathrm{PG}(rt-1,q)$ is the projection of one of the two systems of a Segre variety $\mathcal{S}_{k-1,t-1}$ from a $(kt-rt-1)$-dimensional space $\overline{\Omega^*}$ skew from $\mathcal{S}_{k-1,t-1}$ and $\overline{\Omega}$ and vice versa.*

Proof. Apply field reduction to the spaces Ω^*, Σ^* and Σ in Theorem 4.4 and use Theorem 2.4. □

In the previous corollary, we have seen that $\mathcal{B}(\pi)$ is a projection of a Segre variety (this projection is not necessarily injective). Projections of Segre varieties are studied by Zanella in [55], where he shows that every embedded *product space* is the injective projection of a Segre variety. In [28], the authors investigate the embedding of the product space $\mathrm{PG}(n-1,q) \times \mathrm{PG}(n-1,q)$ in $\mathrm{PG}(2n-1,q)$ and show that $\mathcal{B}(W)$, where W is a scattered subspace of rank n is an embedding of the product space $\mathrm{PG}(n-1,q) \times \mathrm{PG}(n-1,q)$. This embedding is of course covered by two systems of $(n-1)$-dimensional subspaces. However, they prove that $\mathcal{B}(W)$ contains n systems of $(n-1)$-dimensional subspaces, and hence for $n > 2$, contrary to what one might expect, there exist systems of maximum subspaces which are not the image of maximum subspaces of the Segre variety.

4.3 The equivalence of linear sets

A very natural question for linear sets is that of *equivalence*. We say that two sets S_1 and S_2 of points in $\mathrm{PG}(n,q^t)$ are $\mathrm{P\Gamma L}$-equivalent (resp. PGL-equivalent) if there is an element ϕ in $\mathrm{P\Gamma L}(n+1,q^t)$ (resp. $\mathrm{PGL}(n+1,q^t)$) such that $\phi(S_1) = S_2$. In the previous section, we have seen that a linear set can be seen as the projection of a subgeometry. Subgeometries of the same order (embedded in the same projective space) are always PGL-equivalent, but the equivalence problem for projections of subgeometries turns out to be quite hard. The following theorem shows how the equivalence of linear sets, obtained as the projection of a subgeometry, can be translated into the equivalence of the spaces we are projecting from. For the particular case of $\mathbb{F}_q$-linear sets of rank $n+1$ in $\mathrm{PG}(2,q^n)$ (which is the case of linear blocking sets) this was proven in [8].

Theorem 4.6. *[30, Theorem 3] Let S_i be the $\mathbb{F}_q$-linear set of rank r in $\mathrm{PG}(n-1,q^t)$, defined as the projection of $\Sigma_i \cong \mathrm{PG}(r-1,q)$ in Σ^*/Ω_i^*, where $\langle \Sigma_i \rangle = \Sigma^* \cong \mathrm{PG}(r-1,q^t)$, $i = 1,2$, and suppose that S_i is not a linear set of rank s with $s < r$. The following statements are equivalent.*

(i) There exists an element $\alpha \in \mathrm{P\Gamma L}(n,q^t)$ such that $S_1^\alpha = S_2$.

(ii) There exists an element $\beta \in \mathrm{Aut}(\Sigma^*)$ such that $\Sigma_1^\beta = \Sigma_2$ and $(\Omega_1^*)^\beta = \Omega_2^*$.

(iii) For all subgeometries $\Sigma \cong \mathrm{PG}(r-1,q)$ *in* Σ^**, skew to* Ω_1^* *and* Ω_2^**, there exist elements* $\delta, \varphi, \psi \in \mathrm{Aut}(\Sigma^*)$*, such that* $\Sigma^\delta = \Sigma$ *and* $(\Omega_1^*)^{\varphi\delta} = (\Omega_2^*)^\psi$*,* $\Sigma_1^\varphi = \Sigma$ *and* $\Sigma_2^\psi = \Sigma$*.*

In this way, instead of studying the equivalence of linear sets directly, one can study the stabiliser in $\mathrm{P\Gamma L}(r,q^t)$ of a subgeometry $\mathrm{PG}(r-1,q)$ in $\mathrm{PG}(r-1,q^t)$: orbits of this group on subspaces of $\mathrm{PG}(r-1,q^t)$ are in one to one correspondence with $\mathrm{P\Gamma L}$-equivalence classes of the linear sets obtained by projecting from these subspaces.

For the particular case of linear sets of rank 3 in $\mathrm{PG}(1,q^t)$, this reduces to the study of the orbits on points outside π of the stabiliser of a subplane $\pi \cong \mathrm{PG}(2,q)$ in $\mathrm{PG}(2,q^t)$. Let us denote a linear set of size q^2+1 in $\mathrm{PG}(1,q^t)$ by a *club*. A scattered linear set of rank 3 is a linear set containing q^2+q+1 points. The equivalence problem for linear sets of rank 3 is solved in the following theorem.

Theorem 4.7. *[30, Theorem 5]*

(i) All clubs in $\mathrm{PG}(1,q^3)$ *and all scattered linear sets of rank* 3 *in* $\mathrm{PG}(1,q^3)$ *are projectively equivalent.*

(ii) All scattered linear sets of rank 3 *in* $\mathrm{PG}(1,q^4)$ *are projectively equivalent.*

(iii) All clubs and all scattered linear sets of rank 3 *in* $\mathrm{PG}(1,2^5)$ *are equivalent, but there exist projectively inequivalent clubs and projectively inequivalent scattered linear sets of rank* 3 *in* $\mathrm{PG}(1,2^5)$*.*

(iv) In all other cases, there exist non-equivalent clubs and non-equivalent scattered linear sets of rank 3*.*

One can ask whether it is possible to translate the equivalence problem for linear sets $\mathcal{B}(\pi)$ and $\mathcal{B}(\pi')$, where π and π' are subspaces of $\mathrm{PG}(nt-1,q)$ in terms of equivalence of the subspaces π and π'. This problem is still unsolved; we will give an idea why the 'naive' approach is unsuccesful.

Let $S_1 = \mathcal{B}(\pi_1)$ and $S_2 = \mathcal{B}(\pi_2)$ be two $\mathbb{F}_q$-linear sets in $\mathrm{PG}(n-1,q^t)$ and let ϕ be an element of $\mathrm{P\Gamma L}(n,q^t)$ mapping S_1 onto S_2. For all points P of π_1 of weight 1, it is natural to define $\bar{\phi}(P)$ as the unique point P' of π_2 such that $\mathcal{B}(P') = \phi(\mathcal{B}(P))$. Unfortunately, it turns out that this mapping $\bar{\phi}$ cannot always be extended to a collineation of $\mathrm{PG}(nt-1,q)$, as follows from the following theorem.

Theorem 4.8. *[30] Let* $\mathcal{B}(\pi)$ *be a scattered linear set of rank* 3 *in* $\mathrm{PG}(1,q^3)$*,* $q>4$*. Let* P *be a point of* π*. Then there is exactly one plane* $\pi' \neq \pi$ *through* P *such that* $\mathcal{B}(\pi) = \mathcal{B}(\pi')$*.*

Remark 2. Note that the planes π and π' are contained in the hypersurface $\mathcal{Q}_{2,q}$, which was studied in [28]. We refer to [28] for more on this hypersurface and interesting hypersurfaces associated to scattered linear sets in higher dimensions.

Let $\mathcal{B}(\pi)$ be a scattered linear set of rank 3 in $\mathrm{PG}(1,q^3)$, $q>4$ and let P be a point of π. The mapping $\bar{\phi}$ corresponding to the identity element of $\mathrm{P\Gamma L}(2,q^3)$, mapping $\mathcal{B}(\pi)$ onto itself cannot map a line of π through P onto a line of the plane π' through P obtained in Theorem 4.8, since this would imply that there are two transversal lines through P to the same regulus. Hence, $\bar{\phi}$ cannot be extended to a collineation of $\mathrm{PG}(5,q)$.

It can be shown that the points of a line of π are mapped by $\bar{\phi}$ onto the points of a conic in π'; the q^2+q+1 conics obtained in this way form a *bundle of conics*.

4.4 The intersection of linear sets

As seen before, subgeometries provide examples of linear sets. The study of the *intersection* of two subgeometries started in 1980 when Bose, Freeman and Glynn determined the possibilities for the intersection of two Baer subplanes in $\mathrm{PG}(2,q)$ [9]. In 2003, Jagos, Kiss and Pór settled the case of intersecting Baer subgeometries in $\mathrm{PG}(n,q)$ [20]. The problem of the intersection of subgeometries was solved in general by Donati and Durante in 2008, [12] where they proved the following.

Theorem 4.9. *[12, Theorem 1.3] Let G and G' be two subgeometries of order p^t and $p^{t'}$ respectively of $\mathrm{PG}(n,q)$, $q=p^h$, with $t\leq t'$ and let $m=\gcd(t,t')$. If $G\cap G'$ is non-empty, then $G\cap G'=G_1\cup\ldots\cup G_k$, with $k\leq\frac{q-1}{p^{t'}-1}$ and with $G_1,\ldots,G_k$ subgeometries of order p^m of independent subspaces of $\mathrm{PG}(n,q)$.*

They also showed the converse:

Theorem 4.10. *[12, Theorem 1.4] Let t and t' be two positive divisors of h with $t|t'$. Let $k\leq\min\{n+1,\frac{q-1}{p^{t'}-1}\}$ and let $G_1,\ldots,G_k$ be subgeometries of order p^t of independent subspaces of $\mathrm{PG}(n,q)$, $q=p^h$. Then there exist two subgeometries G and G' of order p^t and $p^{t'}$, respectively, of $\mathrm{PG}(n,q)$ such that $G\cap G'=G_1\cup\ldots\cup G_k$.*

The intersection of linear sets in general is considerably more difficult: in general, it is not the union of linear sets contained in independent subspaces and the intersection problem is far from being solved.

The intersection of an *$\mathbb{F}_q$-subline* (which can be seen as an $\mathbb{F}_q$-linear set of rank 2 with $q+1$ points) and a club of $\mathrm{PG}(1,q^t)$ was first determined in [13] by Fancsali and Sziklai. However, in this proof, the authors used that all clubs of $\mathrm{PG}(1,q^t)$ are projectively equivalent, which is in general not true (see Theorem 4.7); in [14], the authors provide a correct proof.

By the following theorem, the intersection problem for an $\mathbb{F}_q$-subline and a linear set is completely solved.

Theorem 4.11. *[30, Theorem 8 and 9] An $\mathbb{F}_q$-subline intersects an $\mathbb{F}_q$-linear set of rank k of $\mathrm{PG}(1,q^h)$ in $0,1,\ldots,\min\{q+1,k\}$ or $q+1$ points and for every subline $L\cong\mathrm{PG}(1,q)$ of $\mathrm{PG}(1,q^h)$, there is a linear set S of rank k, $k\leq h$ and $k\leq q+1$, intersecting L in exactly j points, for all $0\leq j\leq k$.*

This theorem was later extended by Pepe where she determines an upper bound on the size of the intersection of an $\mathbb{F}_{q^s}$-subline and a linear set. Note that, opposed to the case where $s=1$, this theorem does not show that all possibilities occur.

Theorem 4.12. *[38, Proposition 5] An $\mathbb{F}_q$-linear set L of $\mathrm{PG}(1,q^t)$ either contains a fixed subline $\mathrm{PG}(1,q^s)$, $s|t$, or it intersects it in at most $\frac{t}{s}(q^{s-1}+q^{s-2}+\cdots+1)$ points.*

The following theorem deals with the slightly more general case of the intersection of two linear sets of rank 3 in $\mathrm{PG}(1,q^t)$. But as mentioned before, the general problem remains wide open.

Theorem 4.13. *[30, Theorem 23 and Remark 24] Two $\mathbb{F}_q$-linear sets of rank 3 in $\mathrm{PG}(1,q^h)$, $q>3$, intersect in at most $2q+2$ points if q is odd, and in at most $2q+3$ points if q is even. For general q, there are two linear sets of rank 3 in $\mathrm{PG}(1,q^t)$ intersecting in exactly $2q+2$ points.*

4.5 Scattered linear sets and pseudoreguli

We focus on scattered $\mathbb{F}_q$-linear sets of rank $3r$ in $\mathrm{PG}(2r-1,q^3)$. By Theorem 4.2, these scattered linear sets are *maximum scattered*. In this subsection, we will describe the relationship between scattered linear sets and pseudoreguli.

First, it is worth noticing that all maximum scattered linear sets in $\mathrm{PG}(2r-1,q^3)$ are PΓL-equivalent (this was shown for $r=2$ in [37, Proposition 2.7] and for general r in [31, Theorem 4]), whereas in $\mathrm{PG}(2r-1,q^t)$, $t>4$, there exist inequivalent maximum scattered linear sets (see Theorem 4.16).

Let $\mathcal{L}$ be a scattered $\mathbb{F}_q$-linear set of rank $3r$ in $\mathrm{PG}(2r-1,q^3)$, then it can be shown (see [31, Lemma 5]) that a line of $\mathrm{PG}(2r-1,q^3)$ meets $\mathcal{L}$ in $0,1,q+1$ or q^2+q+1 points and every point of $\mathcal{L}$ lies on exactly one (q^2+q+1)-secant to $\mathcal{L}$. Two different (q^2+q+1)-secants to $\mathcal{L}$ are disjoint and there exist exactly two $(r-1)$-spaces, called transversal spaces, meeting each of the (q^2+q+1)-secants. In the spirit of the pseudoregulus defined by Freeman in [15], and extending the definition in [37], the *pseudoregulus* $\mathcal{P}$ associated with $\mathcal{L}$ is defined as the set $\mathcal{P}$ of $\frac{q^{3r}-1}{q^3-1}$ lines meeting $\mathcal{L}$ in q^2+q+1 points.

The following theorem gives a geometric characterisation of a regulus and pseudoregulus.

Theorem 4.14. *[31, Theorem 24] Let $q>2$. Let $\tilde{\mathcal{S}}$ be the point set of a set $\mathcal{S}$ of q^3+1 mutually disjoint lines in $\mathrm{PG}(3,q^3)$ such that the subline defined by three collinear points of $\tilde{\mathcal{S}}$ is contained in $\tilde{\mathcal{S}}$, then $\mathcal{S}$ is a regulus or a pseudoregulus.*

We have seen that there is a pseudoregulus associated to every maximum scattered linear set in $\mathrm{PG}(2r-1,q^3)$. A maximum scattered linear set in $\mathrm{PG}(2r-1,q^t)$ has rank rt, but if $t>3$, we can not in general associate a pseudoregulus to it. For this reason, it makes sense to define maximum scattered linear sets *of pseudoregulus type*. Let L be a scattered $\mathbb{F}_q$-linear set of $\Lambda=\mathrm{PG}(2r-1,q^t)$ of rank rt, $r,t\geq 2$, we say that L is of pseudoregulus type if

(i) there exists $m=\frac{q^{rt}-1}{q^t-1}$ pairwise disjoint lines of Λ, say $s_1,s_2,\ldots,s_m$ such that

$$|L\cap s_i| = q^{t-1}+q^{t-2}+\ldots+q+1, \quad \forall i=1,\ldots,m;$$

(ii) there exist exactly two $(r-1)$-dimensional subspaces T_1 and T_2 of Λ disjoint from L such that $T_j\cap s_i\neq\emptyset$ for each $i=1,\ldots,m$ and $j=1,2$.

The following theorem shows that this family of linear sets is not empty by constructing a family of linear sets $L_{\rho,f}$ that are maximum scattered and of pseudoregulus type.

Theorem 4.15. *[35] Let $T_1=\mathrm{PG}(U_1,\mathbb{F}_{q^t})$ and $T_2=\mathrm{PG}(U_2,\mathbb{F}_{q^t})$ be two disjoint $(r-1)$-dimensional subspaces of $\Lambda=\mathrm{PG}(V,\mathbb{F}_{q^t})=\mathrm{PG}(2r-1,q^t)$ $(t>1)$ and let Φ_f be the semilinear collineation between T_1 and T_2, induced by the invertible semilinear map $f=U_1\to U_2$ having as companion automorphism an element $\sigma\in Aut(\mathbb{F}_{q^t})$ such that $Fix(\sigma)=\mathbb{F}_q$. Then, for each $\rho\in\mathbb{F}_{q^t}^*$, the set*

$$L_{\rho,f}=\{\langle u+\rho f(u)\rangle_{q^t} : u\in U_1\setminus\{0\}\}$$

is an $\mathbb{F}_q$-linear set of Λ of pseudoregulus type whose associated pseudoregulus is $\mathcal{P}_{L_{\rho,f}}=\{\langle P,P^{\Phi_f}\rangle_{q^t} : P\in T_1\}$, with transversal spaces T_1 and T_2.

The authors also count the number of non-equivalent linear sets in the families $L_{\rho,f}$. Here, $\phi(t)$ denotes the Euler ϕ-function, i.e. $\phi(t)$ is the number of integers s smaller than t and relatively prime to t.

Theorem 4.16. *[35] In the projective space $\Lambda = \mathrm{PG}(2r-1, q^t)$ $(r \geq 2, t \geq 3)$ there are $\phi(t)/2$ orbits of scattered $\mathbb{F}_q$-linear sets of Λ of rank rt of type $L_{\rho,f}$ under the action of the collineation group of Λ.*

Linear sets of pseudoregulus type are also studied because of the connection between linear sets and *semifields*, which will be discussed in Section 6.

5 Blocking sets and field reduction

A *blocking set* in $\mathrm{PG}(n,q)$ *with respect to k-spaces* is a set B of points such that every k-dimensional space in $\mathrm{PG}(n,q)$ contains at least one point of B. If we are considering blocking sets with respect to hyperplanes, we simply say that B is a *blocking set*. A *minimal* blocking set B (w.r.t. k-spaces) is a blocking set such that no proper subset of B is a blocking set (w.r.t. k-spaces). A *small* blocking set in $\mathrm{PG}(n,q)$ with respect to k-spaces is a blocking set of size smaller then $3(q^{n-k}+1)/2$. A blocking set B in $\mathrm{PG}(n,q)$ with respect to k-spaces is of Rédei-type if there is a hyperplane containing $|B| - q^{n-k}$ points.

Linear blocking sets with respect to $(k-1)$-spaces in $\mathrm{PG}(n-1,q^t)$ were introduced by Lunardon [33]: he argues that an $\mathbb{F}_q$-linear set of rank $nt-kt+1$ is a blocking set with respect to $(k-1)$-spaces. This can easily be seen: let $\mathcal{B}(\pi)$ be an $\mathbb{F}_q$-linear set in $\mathrm{PG}(n-1,q^t)$, where π is $(nt-kt)$-dimensional, then every $(kt-1)$-dimensional subspace of $\mathrm{PG}(nt-1,q)$ meets π non-trivially, hence, the $(kt-1)$-spaces that arise from applying field reduction to the points of a $(k-1)$-space of $\mathrm{PG}(n-1,q^t)$ meet π, so $\mathcal{B}(\pi)$ is a blocking set w.r.t $(k-1)$-spaces.

Polito and Polverino [39] showed that one can construct *minimal* linear blocking sets in $\mathrm{PG}(2,p^t)$, p prime, $t \geq 4$ that are not of Rédei-type. This contradicted a widespread conjecture which stated that a small minimal blocking set in $\mathrm{PG}(2,q^t)$ would necessarily be of Rédei-type.

Soon after it was proven that there are small minimal linear blocking sets that are not of Rédei-type, people conjectured that all small minimal blocking sets should be linear sets. This conjecture was stated formally by Sziklai in 2008 [48]. Up to our knowledge, this is the complete list of cases in which the linearity conjecture for blocking sets in $\mathrm{PG}(n,p^t)$, p prime w.r.t. k-spaces has been proven.

- $t=1$ (for $n=2$, see [5]; for $n>2$, $k=n-1$, see [18]; for $n>2$, $k\neq n-1$, see [47])
- $t=2$ (for $n=2$, see [46]; for $n>2$, $k=n-1$, see [45]; for $n>2$, $k\neq n-1$, see [54])
- $t=3$ (for $n=2$, see [40]; for $n>2$, $k=n-1$, see [45]; for $n>2$, $k\neq n-1$, see [29, 17])
- $k=n-1$ and B is of Rédei-type (for $n=2$, see [3, 6]; for $n>2$, see [44])

- $k = n - 1$ and $\dim\langle B\rangle = t - 1$ (see [49])
- $k = n - 1$ and $\dim\langle B\rangle = t$ (see [47]).

It is shown in [52] that, loosely speaking, if the linearity conjecture holds in $\mathrm{PG}(2, p^t)$, then it also holds for blocking sets with respect to k-spaces in $\mathrm{PG}(n, p^t)$, provided that p is large enough.

When looking at the construction of a linear blocking set B in $\mathrm{PG}(n-1, q^t)$ with respect to $(k-1)$-spaces, we see that we take B to be $\mathcal{B}(\pi)$, where π is an $(nt - kt)$-space in $\mathrm{PG}(nt-1, q)$, which is a blocking set with respect to $(kt-1)$-spaces. It is clear that every point set $\mathcal{B}(B')$, where B' is a blocking set with respect to $(kt-1)$-spaces in $\mathrm{PG}(nt-1, q)$ is a blocking set with respect to $(k-1)$-spaces in $\mathrm{PG}(n-1, q^t)$. However, the difficulty lies in distinguishing when the obtained blocking set is minimal. The following theorem provides us with one case in which the minimality of $\mathcal{B}(B')$ can be proven. Note that a semioval is a set S of points such that every point of S lies on a unique tangent line to S.

Theorem 5.1. *[51] Let Ω be an $(nt - kt - 2)$-dimensional subspace of $\mathrm{PG}(nt - 1, q)$, let $\bar{B}$ be a minimal blocking set that is not a semioval, contained in the plane Γ which is skew from Ω and let K be the cone with vertex Ω and base $\bar{B}$. Let $B = \mathcal{B}(K)$, then B is a minimal blocking set with respect to $(k-1)$-spaces in $\mathrm{PG}(n-1, q^t)$.*

If we take $\bar{B}$ in the previous theorem to be a line, then the constructed blocking set is a linear blocking set and we may conclude that a linear blocking set is indeed minimal. For blocking sets with respect to lines in $\mathrm{PG}(n-1, q^t)$ this was already shown in [34] and for $k \neq n-1$, we could deduce the minimality of a linear blocking set from [47, Lemma 3.1].

6 Semifields and linear sets

Finite semifields are a generalisation of finite fields (where associativity of multiplication is not assumed) and the study of linear sets and field reduction has been shown very useful in this theory.

A *finite semifield* $(\mathbb{S}, +, \circ)$ is an algebra of finite dimension over a finite field $\mathbb{F}$ with at least two elements, and two binary operations $+$ and $\circ$, satisfying the following axioms.

(S1) $(\mathbb{S}, +)$ is a group with identity element 0.

(S2) $x \circ (y + z) = x \circ y + x \circ z$ and $(x + y) \circ z = x \circ z + y \circ z$, for all $x, y, z \in \mathbb{S}$.

(S3) $x \circ y = 0$ implies $x = 0$ or $y = 0$.

(S4) $\exists 1 \in \mathbb{S}$ such that $1 \circ x = x \circ 1 = x$, for all $x \in \mathbb{S}$.

Without axiom (S4) we have the definition of a *pre-semifields*.

Semifields are usually studied up to isotopism, because of the one-to-one correspondence between the isotopism classes of semifields and the isomorphism classes of the associated projective planes (by a theorem of A. A. Albert). An *isotopism* (or *isotopy*)

between two (pre-)semifields $(\mathbb{S}, \circ)$ and $(\mathbb{S}', \circ')$ is a triple (F, G, H) of nonsingular linear maps from $\mathbb{S}$ to $\mathbb{S}'$ such that

$$x^F \circ' y^G = (x \circ y)^H,$$

for all $x, y \in \mathbb{S}$. If such an isotopism exists, the (pre-)semifields $\mathbb{S}$ and $\mathbb{S}'$ are called *isotopic* and the isotopism class of a (pre-)semifield $\mathbb{S}$ is denoted by $[\mathbb{S}]$.

The nuclei of a semifield are associative substructures of a semifield, and they arise in a similar way as the (commutative) center of non-commutative algebraic structures. However, while the commutative center is uniquely defined for a non-commutative structure, there are four different associative substructures to consider for non-associative structures. These are called the nucleus, the left nucleus, the middle nucleus, and the right nucleus and are defined as follows.

The subset

$$\mathbb{N}_l(\mathbb{S}) := \{x \ : \ x \in \mathbb{S} \mid x \circ (y \circ z) = (x \circ y) \circ z, \ \forall y, z \in \mathbb{S}\},$$

is called the *left nucleus* of $\mathbb{S}$. Analogously, one defines the *middle nucleus*

$$\mathbb{N}_m(\mathbb{S}) := \{y \ : \ y \in \mathbb{S} \mid x \circ (y \circ z) = (x \circ y) \circ z, \ \forall x, z \in \mathbb{S}\},$$

and the *right nucleus*

$$\mathbb{N}_r(\mathbb{S}) := \{z \ : \ z \in \mathbb{S} \mid x \circ (y \circ z) = (x \circ y) \circ z, \ \forall x, y \in \mathbb{S}\}.$$

The intersection of these three nuclei is called the *nucleus* or *associative center* $\mathbb{N}(\mathbb{S})$, while the intersection of the associative center and the *commutative center* $C(\mathbb{S})$ (defined in the usual way) is called the *center* of $\mathbb{S}$ and denoted by $Z(\mathbb{S})$. One easily verifies that all of these substructures are finite fields and $\mathbb{S}$ can be seen as a (left or right) vectorspace over these substructures, e.g. as a left vector space $V_l(\mathbb{S})$ over its left nucleus. Right multiplication in $\mathbb{S}$ by an element x is denoted by R_x, i.e. $y^{R_x} = y \circ x$, which is an endomorphism of $V_l(\mathbb{S})$.

We can now explain the geometric approach to finite semifields, which has been very fruitful in recent years.

This approach naturally breaks up the study of semifields into different cases depending on the parameters of the semifield. Here we only give the correspondence theorem in the general setting, where no assumptions on the nuclei or other properties of the semifield are made.

Let $\mathbb{S}$ be an n-dimensional semifield over $\mathbb{F}_q$, and denote the dimensions of $\mathbb{S}$ over its left nucleus by l. We define the following subspaces of $\mathbb{S} \times \mathbb{S}$. For each $x \in \mathbb{S}$, consider the set of vectors $S_x := \{(y, y^{R_x}) : y \in \mathbb{S}\}$, and put $S_\infty := \{(0, y) : y \in \mathbb{S}\}$. Then $\mathcal{S} := \{S_x : x \in \mathbb{S}\} \cup \{S_\infty\}$ is a spread of $\mathbb{S} \times \mathbb{S}$. The set of endomorphisms $\mathcal{R} := \{R_x \ : \ x \in \mathbb{S}\} \subset \mathrm{End}(V_l(\mathbb{S}))$ is called the *semifield spread set* corresponding to $\mathbb{S}$. Note that by (S2) the spread set $\mathcal{R}$ is closed under addition and, by (S3), the non-zero elements of $\mathcal{R}$ are invertible.

This means that n-dimensional semifields over $\mathbb{F}_q$, can be investigated via the $\mathbb{F}_q$-vector space $U \subset \mathbb{F}_q^{ln}$ of dimension n induced by the $\mathbb{F}_q$-vector space $\mathcal{R} \subset \mathrm{End}(V_l(\mathbb{S}))$. Projectively this corresponds to the study of the $\mathbb{F}_q$-linear set $L(\mathbb{S}) := B(U)$ of rank n in $\mathrm{PG}(l^2-1, q^{n/l}) = \mathrm{PG}(V_l(\mathbb{S}))$. This leads us to the general correspondence theorem, which allows us to use the geometric properties of linear sets in relation to the Segre variety, to solve isotopism problems for finite semifields.

Theorem 6.1 ([24]). *Let $\mathcal{S}_{l,l}(q^{n/l})$ denote the Segre variety in $\mathrm{PG}(l^2-1,q^{n/l})$, and denote its $(l-2)$nd secant variety by Ω. Let $\mathcal{G}$ denote the stabiliser inside the collineation group $\mathrm{P\Gamma L}(l^2,q^{n/l})$ of the two families of maximal subspaces on $\mathcal{S}_{l,l}(q^{n/l})$, and let X denote the set of linear sets of rank n disjoint from Ω. Then the isotopism classes of semifields of order q^n, l-dimensional over their left nucleus, are in one-to-one correspondence with the orbits of $\mathcal{G}$ on the set X.*

More details on this approach, the treatment of different special cases and several other links with finite geometry can be found in [37], [27], [25], [35]. The recent paper [26] is a nice illustration of how the study of linear sets of pseudoregulus type associated to certain semifields can be used to solve isotopism problems for these semifields.

References

[1] J. André. Über nicht-Desarguessche Ebenen mit transitiver Translationsgruppe. *Math. Z.* **60** (1954), 156–186.

[2] L. Bader and G. Lunardon. Desarguesian spreads. *Ricerche mat.* **60 (1)** (2011), 15–37.

[3] S. Ball. The number of directions determined by a function over a finite field. *J. Combin. Theory Ser. A* **104 (2)** (2003), 341–350.

[4] A. Barlotti and J. Cofman. Finite Sperner spaces constructed from projective and affine spaces. *Abh. Math. Semin. Univ. Hamb.* **40** (1974), 231–241.

[5] A. Blokhuis. On the size of a blocking set in $\mathrm{PG}(2,p)$. *Combinatorica* **14 (1)** (1994), 111–114.

[6] A. Blokhuis, S. Ball, A.E. Brouwer, L. Storme, and T. Szőnyi. On the number of slopes of the graph of a function defined on a finite field. *J. Combin. Theory Ser. A* **86 (1)** (1999), 187–196.

[7] A. Blokhuis and M. Lavrauw. Scattered spaces with respect to a spread in $\mathrm{PG}(n,q)$. *Geom. Dedicata* **81 (1-3)** (2000), 231–243.

[8] G. Bonoli and O. Polverino. $\mathbb{F}_q$-linear blocking sets in $\mathrm{PG}(2,q^4)$. *Innov. Incidence Geom.* **2** (2005), 35–56.

[9] R.C. Bose, J.W. Freeman, and D.G. Glynn. On the intersection of two Baer subplanes in a finite projective plane. *Utilitas Math.* **17** (1980), 65–77.

[10] R.H. Bruck and R.C. Bose. The construction of translation planes from projective spaces. *J. Algebra* **1** (1964), 85–102.

[11] L. R. Casse and C. M. OKeefe. Indicator sets for t-spreads of $\mathrm{PG}((s+1)(t+1)-1,q)$. *Boll. Un. Mat. Ital. B* **7 (4)** (1990), 13–33.

[12] G. Donati and N. Durante. On the intersection of two subgeometries of $\mathrm{PG}(n,q)$. *Des. Codes Cryptogr.* **46 (3)** (2008), 261–267.

[13] Sz.L. Fancsali and P. Sziklai. About maximal partial 2-spreads in PG$(3m-1,q)$. *Innov. Incidence Geom.* **4** (2006), 89–102.

[14] Sz.L. Fancsali and P. Sziklai. Description of the clubs. *Ann. Univ. Sci. Budapest. Eötvös Sect. Math.* **51** (2009), 141–146.

[15] J.W. Freeman. Reguli and pseudo-reguli in PG$(3,q^2)$. *Geom. Dedicata* **9** (1980), 267–280.

[16] N. Gill. Polar spaces and embeddings of classical groups. *New Zealand J. Math.* **36** (2007), 175–184.

[17] N.V. Harrach, K. Metsch, T. Szőnyi, and Zs. Weiner. Small point sets of PG(n,p^{3h}) intersecting each line in 1 mod p^h points. *J. Geom.* **98 (1–2)** (2010), 59–78.

[18] U. Heim. Proper blocking sets in projective spaces. *Discrete Math.* **174 (1–3)** (1997), 167–176.

[19] J.W.P. Hirschfeld and J.A. Thas. *General Galois Geometries*. Oxford University Press, Oxford, 1991.

[20] I. Jagos, G. Kiss, and A. Pór. On the intersection of Baer subgeometries of PG(n,q^2). *Acta Sci. Math.* **69 (1–2)** (2003), 419–429.

[21] S. Kelly. Constructions of intriguing sets of polar spaces from field reduction and derivation. *Des. Codes Cryptogr.* **43 (1)** (2007), 1–8.

[22] P. Kleidman and M. Liebeck. *The Subgroup Structure of the Finite Classical Groups.* Cambridge University Press, Cambridge, 1990.

[23] M. Lavrauw. Scattered spaces with respect to spreads, and eggs in finite projective spaces. PhD Dissertation, Eindhoven University of Technology, Eindhoven, 2001.

[24] M. Lavrauw. Finite semifields with a large nucleus and higher secant varieties to Segre varieties. Adv. Geom. **11** (2011), 399–410.

[25] M. Lavrauw. Finite semifields and nonsingular tensors. *Des. Codes Cryptogr.* **68**, 1-3 (2013), 205–227.

[26] M. Lavrauw, G. Marino, O. Polverino and R. Trombetti. Solution to an isotopism question concerning rank 2 semifields. To appear in *Journal of Combinatorial Designs*.

[27] M. Lavrauw and O. Polverino O. *Finite semifields and Galois geometry*. Chapter in: De Beule J., Storme L. (eds.) Current Research Topics in Galois Geometry. NOVA Academic Publishers, 2011.

[28] M. Lavrauw, J. Sheekey and C. Zanella. On embeddings of minimum dimension of PG$(n,q)\times$PG(n,q). To appear in *Des. Codes Cryptogr.*

[29] M. Lavrauw, L. Storme and G. Van de Voorde. A proof of the linearity conjecture for k-blocking sets in $\mathrm{PG}(n, p^3)$, p prime. *J. Combin. Theory, Ser. A* **118 (3)** (2011), 808–818.

[30] M. Lavrauw and G. Van de Voorde. On linear sets on a projective line. *Des. Codes Cryptogr.* **56 (2-3)** (2010), 89–104.

[31] M. Lavrauw and G. Van de Voorde. Scattered linear sets and pseudoreguli. *Electronic J. Combin* **20 (1)** (2013), P15.

[32] M. Limbos. A characterisation of the embeddings of $\mathrm{PG}(m, q)$ into $\mathrm{PG}(n, q^r)$. *J. Geom.* **16 (1)** (1981), 50–55.

[33] G. Lunardon. Normal spreads. *Geom. Dedicata* **75 (3)** (1999), 245–261.

[34] G. Lunardon. Linear k-blocking sets. *Combinatorica* **21 (4)** (2001), 571–581.

[35] G. Lunardon, G. Marino, O. Polverino and R. Trombetti. Maximum scattered linear sets of pseudoregulus type and the Segre Variety $\mathcal{S}_{n,n}$. To appear in *J. Algebraic Combin.*

[36] G. Lunardon and O. Polverino. Translation ovoids of orthogonal polar spaces. *Forum Math.* **16 (5)** (2004), 663–669.

[37] G. Marino, O. Polverino, and R. Trombetti. On $\mathbb{F}_q$-linear sets of $\mathrm{PG}(3, q^3)$ and semifields. *J. Combin. Theory, Ser. A* **114 (5)** (2007), 769–788.

[38] V. Pepe. On the algebraic variety $\mathcal{V}_{r,t}$. *Finite Fields Appl.* **17 (4)** (2011), 343–349.

[39] P. Polito and O. Polverino. On small blocking sets. *Combinatorica* **18 (1)** (1998), 133–137.

[40] O. Polverino. Small blocking sets in $\mathrm{PG}(2, p^3)$. *Des. Codes Cryptogr.* **20 (3)** (2000), 319–324.

[41] O. Polverino. Linear sets in finite projective spaces. *Discrete Math.* **310 (22)** (2010), 3096–3107.

[42] B. Segre. Teoria di Galois, fibrazioni proiettive e geometrie non desarguesiane. *Ann. Mat. Pura Appl.* **64** (1964), 1–76.

[43] E.E. Shult and J. Thas. m-systems of polar spaces. *J. Combin. Theory Ser. A* **68 (1)** (1994), 184–204.

[44] L. Storme and P. Sziklai. Linear pointsets and Rédei type k-blocking sets in $\mathrm{PG}(n, q)$. *J. Algebraic Combin.* **14 (3)** (2001), 221–228.

[45] L. Storme and Zs. Weiner. On 1-blocking sets in $\mathrm{PG}(n, q)$, $n \geq 3$. *Des. Codes Cryptogr.* **21 (1–3)** (2000), 235–251.

[46] T. Szőnyi. Blocking sets in desarguesian affine and projective planes. *Finite Fields Appl.* **3 (3)** (1997), 187–202.

[47] T. Szőnyi and Zs. Weiner. Small blocking sets in higher dimensions. *J. Combin. Theory, Ser. A* **95 (1)** (2001), 88–101.

[48] P. Sziklai. On small blocking sets and their linearity. *J. Combin. Theory, Ser. A* **115 (7)** (2008), 1167–1182.

[49] P. Sziklai and G. Van de Voorde. A small minimal blocking set in $\mathrm{PG}(n, p^t)$, spanning a $(t-1)$-space, is linear. *Des. Codes Cryptogr.* **68 (1-3)** (2013), 25–32.

[50] J. Tits. Buildings of spherical type and finite BN-pairs. *Springer-Verlag, Berlin, Lecture Notes in Mathematics* **386**, 1974.

[51] G. Van de Voorde. Constructing minimal blocking sets using field reduction. Preprint.

[52] G. Van de Voorde. On the linearity of higher-dimensional blocking sets. *Electronic J. Combin.* **17(1)** (2010), Research Paper 174, 16 pp.

[53] F.D. Veldkamp. Polar geometry. *Indag. Math.* **21** (1959), 512–551.

[54] Zs. Weiner. Small point sets of $\mathrm{PG}(n, q)$ intersecting each k-space in 1 modulo $\sqrt{q}$ points. *Innov. Incidence Geom.* **1** (2005), 171–180.

[55] C. Zanella. Universal properties of the Corrado Segre embedding. *Bull. Belg. Math. Soc. Simon Stevin.* **3 (1)** (1996), 65–79.